Claims

What is claimed is:

1. A method for enabling targeted information retrieval while protecting consumer privacy, the method comprising:

(a) providing a plurality of elements of information;

(b) specifying a negotiant function designed to accept a plurality of elements of data associated with a consumer as input and produce an information request as output, said information request designating at least one element of information to present to the consumer from among a plurality of elements of information; and

(c) distributing the negotiant function to a consumer for execution by said consumer.

2. The method of claim 1, the method further comprising, after step (c), the steps of

(d) receiving the information request from said consumer, said information request produced by the negotiant function; and

(e) transmitting the at least one element of information to the consumer in response to the information request.

3. A method for enabling targeted information retrieval while protecting consumer privacy, the method comprising:

(a) receiving a negotiant function for execution, said negotiant function designed to produce an information request as output, the information request designating at least one element of information from among a plurality of elements of information; and

(b) executing said negotiant function to generate the information request.

4. The method of claim 3 wherein said negotiant function is designed to accept a plurality of elements of data associated with a consumer as input.

5. The method of claim 3, the method further comprising, after step (b), the step of transmitting said information request to a source of information.

6. The method of claim 5, the method further comprising, after the transmitting step, the step of receiving at least one element of information from the source of information in response to the information request.

7. A method for enabling targeted information retrieval while protecting consumer privacy by processing aggregated requests, the method comprising:

(a) distributing a negotiant function for execution to a plurality of consumers, the negotiant function designed to produce an information request as output;

(b) receiving a plurality of information requests, a first information request of the plurality of information requests associated with a first consumer and obtained by applying a first negotiant function to an element of data associated with the first consumer, a second information request of the plurality of information requests associated with a second consumer and obtained by applying a second negotiant function to an element of data associated with the second consumer.

8. The method of claim 7, the method further comprising, after step (b), the steps of aggregating a plurality of request pairs, said plurality of request pairs having a sequence, each of said plurality of request pairs comprising an information request and an identifier; and transmitting the plurality of request pairs to a source of information.

9. The method of claim 7, the method further comprising, after step (b), the steps of encrypting the plurality of information requests; and aggregating a plurality of request pairs V_1, said plurality of request pairs having a sequence, each of said plurality of request pairs comprising an encrypted information request and a consumer identifier.

10. The method of claim 9, the method further comprising, the step of applying a mix network to said plurality of request pairs V_1 to obtain a plurality of request pairs V_2, the plurality

of request pairs V_1 having a first sequence, each of the plurality of request pairs V_1 comprising an information request, said information request encrypted with a first public key and a first random encryption factor, and an identifier, the plurality of request pairs V_2 having a second sequence comprising the first sequence permuted by a first random secret permutation, each of the plurality of request pairs V_2 comprising the information request in plaintext and the identifier encrypted with a second public key and a second random encryption factor.

11. The method of claim 10, the method further comprising, the step of replacing the information request in each of the plurality of request pairs V_2 with an element of information to create a plurality of response pairs V_2'.

12. The method of claim 11, the method further comprising, the step of applying a mix network to the plurality of response pairs V_2' to obtain a plurality of response pairs V_3, the plurality of response pairs V_3 having a third sequence comprising the second sequence permuted by a second random secret permutation, each of the plurality of response pairs V_3 comprising the element of information, said element of information encrypted with a third public key and a third random encryption factor, and the identifier in plaintext.

13. The method of claim 12, wherein the first public key, the second public key, and the third public key are a single public key.

14. The method of claim 12, the method further comprising, after step (b), the step of applying asymmetric proxy re-encryption to the plurality of response pairs V_3 to obtain a plurality of response pairs V_4, each of the plurality of response pairs V_4 comprising the element of information encrypted with a fourth public key and the identifier in plaintext.

15. The method of claim 14 the method further comprising, the step of making the element of information encrypted with the fourth public key available to a consumer based on the identifier.

16. The method of claim 14 wherein quorum-controlled asymmetric proxy re-encryption is applied to the plurality of response pairs V_3 to obtain a plurality of response pairs V_4, each of the plurality of response pairs V_4 comprising the element of information encrypted with the fourth public key and the identifier in plaintext.

17. The method of claim 16 wherein the fourth public key is a key of the consumer; and wherein making the element of information encrypted with the fourth key available to the consumer based on the identifier comprises transmitting the element of information encrypted with the fourth public key to the consumer in response to the identifier.

18. A method for targeted information retrieval while protecting consumer privacy by comparing blinded ciphertexts, the method comprising:

(a) distributing a negotiant function for execution to a plurality of consumers, the negotiant function designed to produce an information request as output;

(b) receiving a request pair in response to the negotiant function, the request pair comprising a consumer identifier and the information request and a first random encryption factor, the information request encrypted with the first public key and the first random encryption factor having a first underlying plaintext;

(c) constructing a first plurality of information pairs, the first plurality of information pairs having a first sequence, each of the first plurality of information pairs comprising an element identifier and an element of information encrypted with a second public key and a second random encryption factor;

(d) applying a mix network to the first plurality of information pairs to obtain a second plurality of information pairs, the second plurality of information pairs having a second sequence comprising the first sequence permuted by a random secret permutation, each of the second plurality of request pairs comprising the element identifier encrypted with a third public key and a third random encryption factor and the element of information re-encrypted with the third public key and the third random encryption factor, the element identifier encrypted with the third public key and the third random encryption factor having a second underlying plaintext; and

(e) performing a distributed plaintext equality test to identify at least one of the

second plurality of request pairs in which the second underlying plaintext is identical to the first underlying plaintext.

19. The method of claim 18 wherein the first public key, the second public key, and the third public key are a single public key.

20. The method of claim 18, the method further comprising, after step (e), the step of applying asymmetric proxy re-encryption to the at least one of the second plurality of request pairs in which the second underlying plaintext is identical to the first underlying plaintext to obtain at least one response pair, each of the at least one response pair comprising the element of information encrypted with a fourth public key and the consumer identifier.

21. The method of claim 20 wherein quorum-controlled asymmetric proxy re-encryption is applied to the at least one of the second plurality of request pairs in which the second underlying plaintext is identical to the first underlying plaintext to obtain at least one response pair, each of the at least one response pair comprising the element of information encrypted with the fourth public key and the consumer identifier.

22. The method of claim 21, the method further comprising, after step (e), the step of making the element of information encrypted with the fourth public key available to the consumer based on the consumer identifier.

23. The method of claim 22 wherein the step of making the element of information encrypted with the fourth public key available to the consumer based on the consumer identifier comprises transmitting the element of information encrypted with the fourth public key to the consumer in response to the consumer identifier.